RSA NetWitness Platform

Event Source Log Configuration Guide

NFDump

Last Modified: Monday, November 18, 2019

Event Source Product Information:

Vendor: Sourceforge.net
Event Source: NFDump
Versions: netflow v5, v7, v9, NFDump v1.5.7, 1.6.x
Additional Downloads: nicsftpagent.conf.nfdump, rsa_nfdump

RSA Product Information:
Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: nfdump
Collection Method: File
Event Source Class.Subclass: Network.System

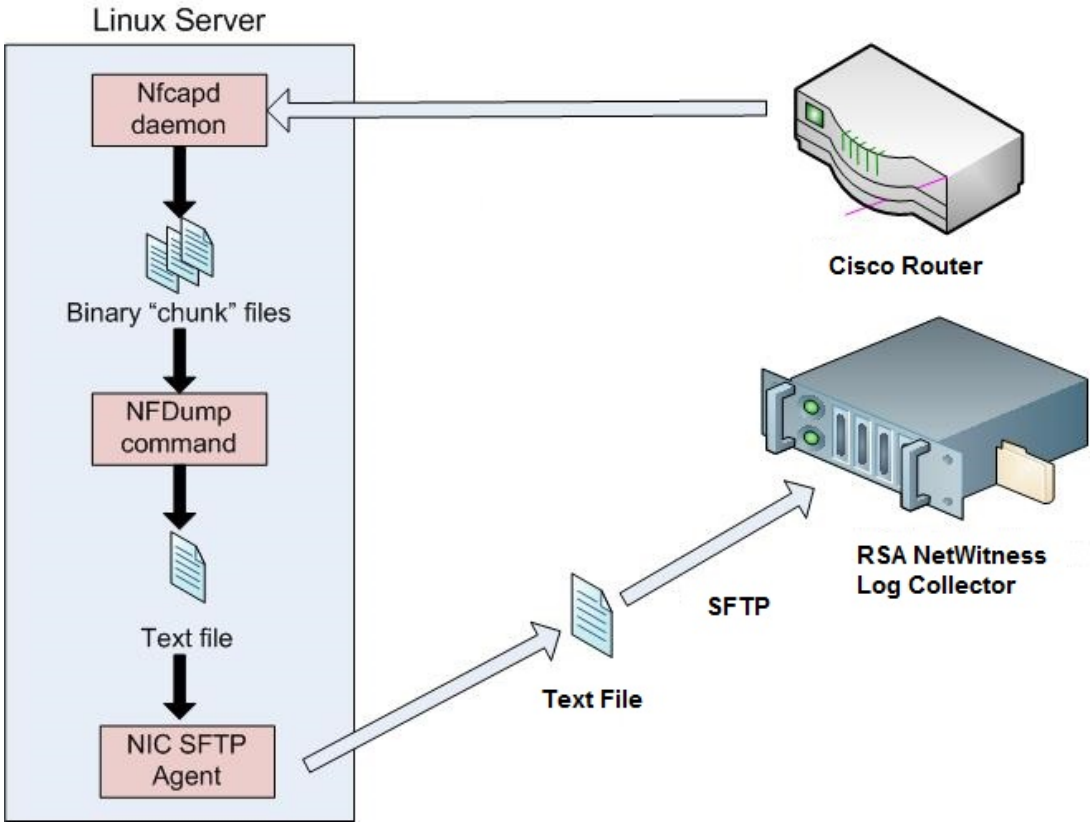
NFDump Overview

NFDump is a set of Open Source tools used to collect and process NetFlow data from Cisco Routers. NFDump supports NetFlow versions v5, v7 and v9 as well as a limited set of sFlow and is IPv6 compatible. The tools reside on a Linux server and collect NetFlow data that is pushed from the router.

The individual tools are the following:

- **nfcapd**, a NetFlow capture daemon. It reads the NetFlow data from the network and stores it in binary files. The daemon creates new files approximately every five minutes.
- **nfdump**, the NetFlow dump command. It reads the NetFlow data from the files stored by **nfcapd**, and outputs them to a text file.

When you use NFDump to capture Cisco router data to RSA NetWitness Platform, the data flows as follows:



The Cisco Router outputs data to the Linux Server, which is running NFDump. The `nfcapd` daemon outputs data into binary files (typically 5-minute chunks). When you run the `nfdump` command, it outputs the binary data into a text file. Then, you use the SFTP protocol to send the data to RSA NetWitness Platform.

NFDump Configuration

To configure NFDump, you must complete these tasks:

I. Configure NFDump to collect NetFlow Data

II. Set up the SFTP Agent

III. Create a Job to Run Periodically

IV. Configure a Cisco router to send NetFlow Data to the NFDump server

V. Configure the RSA NetWitness Platform Log Collector for File Collection

Configure NFDump to collect NetFlow Data

To configure NFDump to collect data:

1. Install NFDump on your Linux server and follow the vendor instructions on the proper installation of NFDump.
2. Create the following directories:

   ```
   /var/log/rsa/nfdump/
   /var/log/rsa/nfdump/rawdata
   /var/log/rsa/nfdump/staging
   /var/log/rsa/nfdump/upload
   ```

3. Add the following line at the end of the server's `/etc/rc.d/rc.local` file:

   ```
   /usr/local/bin/nfcapd -w -D -l /var/log/rsa/nfdump/rawdata -p 9995
   ```

   This command causes **nfcapd** to run (using the defaults) and create the binary data file to hold the data from the Cisco router.

4. Restart the **rc.local** file by running the following command:

   ```
   bash /etc/rc.local
   ```

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see Install and Update SFTP Agent
- To set up the SFTP agent on Linux, see Configure SFTP Shell Script File Transfer

To download NFDump setup files from the RSA Link website:

1. Download the documentation: Configure SA SFTP Agent shell script

   Refer to that document as you complete the following steps.

2. Download the RSA NetWitness Unix SFTP Agent, which is available here: https://community.rsa.com/docs/DOC-45018.

   Note: You need to log on with credentials supplied to you by RSA.

3. Download the sample configuration file. Additional Downloads are available from the the RSA® NetWitness® Platform Event Source Downloads space on RSA Link. The files for NFDump are here:

   https://community.rsa.com/docs/DOC-58020.

4. Click on the **nicsftpagent.conf.nfdump** , and save to **/usr/local/nic/nicsftpagent.conf** (Note that you must rename the file to **nicsftpagent.conf**).

5. Click on the **rsa_nfdump** file, and save to **/var/log/rsa/nfdump/rsa_nfdump**.

6. Refer to the *Configure SA SFTP Agent Shell Script* guide to complete the set up.

Create a Job to Run Periodically

This section describes how to create a job to run periodically to send data to RSA NetWitness Platform.

To create a job to run periodically:

1. Place the following line in the crontab using the **crontab –e** command:

   ```
   5,10,15,20,25,30,35,40,45,50,55,59 * * * * /var/log/rsa/nfdump/rsa_nfdump
   ```

   Note: You can avoid receiving e-mail when there is no NFDump data. To do so, add `>> /dev/null 2>&1` to the end of the crontab:

   ```
   5,10,15,20,25,30,35,40,45,50,55,59 * * * * /var/log/rsa/nfdump/rsa_
   nfdump >> /dev/null 2>&1
   ```

2. Restart the cron service by running the following command:

   ```
   /etc/init.d/crond restart
   ```

Configure a Cisco router to send NetFlow Data to the NFDump server

NetFlow captures data from ingress (incoming) and egress (outgoing) packets and sends them to a collector (NFDump) on the Linux server.

Note: The administrator running the following commands must have the appropriate access to the router.

Use the Cisco IOS command-line interface to configure a Cisco Router:

Note: The following commands provide an example of how to configure a Cisco Router to export the NetFlow data to the NFDump server. Specifically, these commands configure a Cisco 2821 Router; for other routers, the specific commands may vary slightly.

Run the following commands in the order listed:

```
enable
configure terminal
ip flow-export destination ip-address-of-NFDump-Server 9995
interface GigabitEthernet 0/0
ip flow egress
ip flow ingress
exit
exit
copy running-config startup-config
```

Note: For the `ip flow-export destination` command, note that the port number, 9995, must match the port number set when configuring the **nfcapd** command in Task II.

Configure the Log Collector for File Collection

Perform the following steps to configure the Log Collector for File collection.

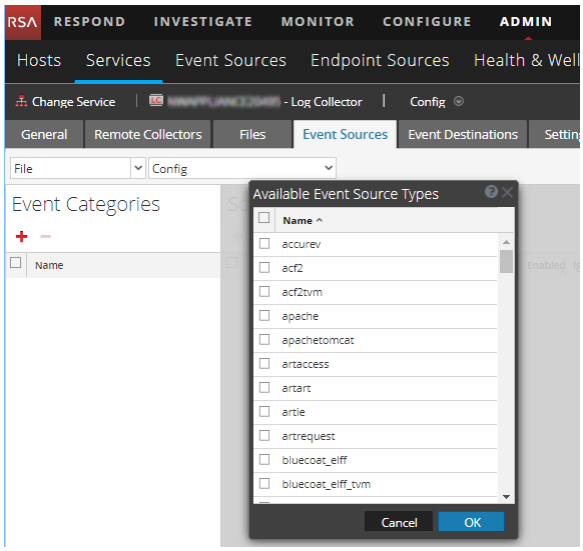
To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **File/Config** from the drop-down menu.

The Event Categories panel displays the File event sources that are configured, if any.

4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.

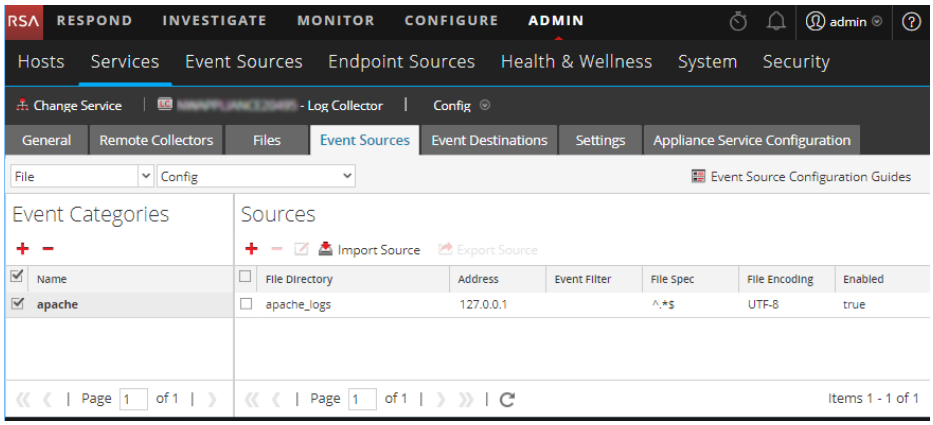


5. Select the correct type from the list, and click **OK**.

   Select **nfdump** from the **Available Event Source Types** dialog.

   The newly added event source type is displayed in the Event Categories panel.

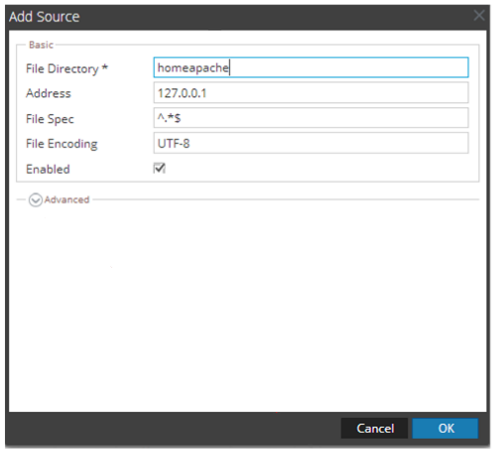
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

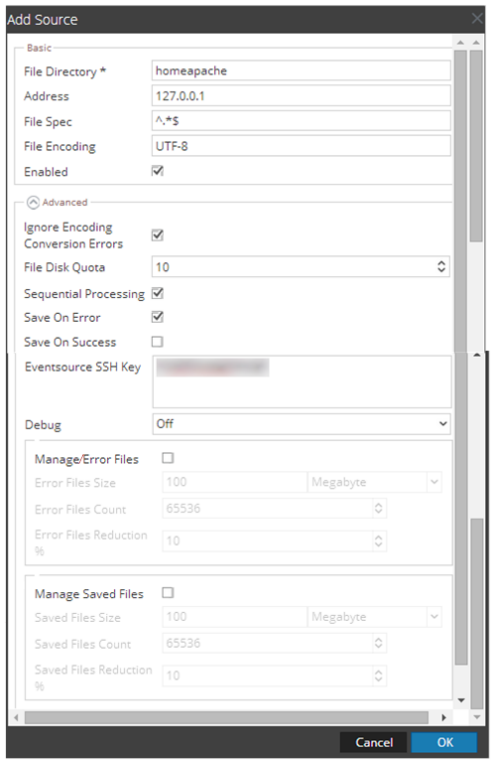


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.

   Note: Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.





7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.

8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.